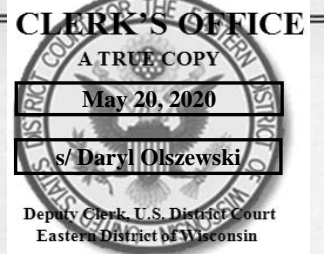


## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Facebook Username: Rios Davito, Facebook  
User ID: 100013585895525

Case No. 20 MJ 134

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the \_\_\_\_\_ District of \_\_\_\_\_, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. Section 1073

Flight to Avoid Prosecution

Offense Description

The application is based on these facts:  
See Attached Affidavit

☐ Continued on the attached sheet.

☒ Delayed notice of 180 days (give exact ending date if more than 30 days: 11/16/2020) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Deputy Clint Blauser, USMS

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone and email \_\_\_\_\_ (specify reliable electronic means)

Date: May 20, 2020

Judge's signature

City and state: Milwaukee, WI

Hon. William E. Duffin

Printed name and title

## **AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT**

I, Clint Blauser, being duly sworn, hereby depose and say:

1. I am a Deputy United States Marshal with the United States Marshals Service (USMS) and, as such, am charged with enforcing all laws in all jurisdictions of the United States, its territories and possessions. I have been a member of the United States Marshals Service for nine years and during that time have been assigned to the U.S. Marshals Fugitive Task Force for over four years. While assigned to the Fugitive Task Force, I have investigated several hundred fugitive cases and have located fugitives utilizing methods in electronic surveillance to include social media accounts.

2. This Affidavit is made in support of an application for a search warrant to search the **Target Account**, more fully described in Attachment A, for evidence and instrumentalities for Flight to Avoid Prosecution, in violation of Title 18, United States Code, Section 1073, and Title 18, United States code, Section 2 (aiding and abetting an offense against the United States).

3. The facts set forth in this Affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement agents and witnesses. This Affidavit is intended to show that there is probable cause to believe that fruits, instrumentalities, and evidence, more fully described in Attachment B, for the subject offense will be found in the **Target Account**, more fully described in Attachment A, and does not purport to set forth all of my knowledge of or investigation into this matter.

### **STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS**

4. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled “Stored Wire and Electronic Communications and Transactional Records Access.”

- a. Title 18, United States Code, Section 2703(a) provides, in part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

- b. Title 18, United States Code, Section 2703(b) provides, in part:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant□.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computer service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

- c. The government may also obtain records and other information pertaining to a subscriber to or customer of electronic communication service or remote computing service by way of a search warrant. See 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. See 18 U.S.C. § 2703(c)(3).

d. The statute permits the warrant to be served on the provider, who will then disclose the relevant records to the officer, who need not be onsite at the time the search is executed. Title 18, United States Code, Section 2703(g), provides, in part:

Presence of Officer Not Required -- Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

e. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system.

f. Title 18, United States Code, Section 2510, provides, in part:

(8) “contents,” when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

(14) “electronic communications system” means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .

(15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications; . . .

(17) “electronic storage” means

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

## FACEBOOK TECHNICAL BACKGROUND

5. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts through which users can share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

6. Facebook asks users to provide basic contact information, either during the registration process or thereafter. This information may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

7. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information in the user's account available only to himself or herself, to other specified Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook. Depending on the user's privacy settings, Facebook may also obtain and store the physical location of the user's device(s) as they interact with the Facebook service on those device(s).

8. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for

purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

9. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

10. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

11. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or

on their own profiles; such comments are typically associated with a specific posting or item on the profile.

12. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

13. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

14. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

15. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and creator of the group. Facebook also assigns a group identification number to each group. Facebook uses the term “Group Contact Info” to describe the contact information for the group’s creator and administrator, as well as the current status of the group profile page.

16. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

17. Facebook also retains IP address logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action.

18. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service used, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications.

19. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers

and their use of Facebook, such as account access information, transaction information, and account application.

### **PROBABLE CAUSE**

20. On January 10, 2020, a criminal complaint (Case No. 20-mj-834 (WEC)) and arrest warrant were issued charging David Quinones-Rios in the Eastern District of Wisconsin and elsewhere with conspiracy to possess with the intent to distribute, controlled substances, in violation of Title 21 U.S.C. Section 846; possession with intent to distribute and distribution of controlled substances in violation of Title 21, United States Code Section 841(a)(1); attempt to possess with intent to distribute and to distribute controlled substances in violation of Title 21, United States Code, Section 846; use of communications facilities to facilitate controlled substance felonies, in violation of Title 21, United States Code Section 843(b), conspiracy to launder monetary instruments in violation of Title 18, United States Code, Section 1956(h); and money laundering in violation of Title 18 United States Code, Sections 1956(a)(1)(B)(i), and 2. On February 11, 2020, a grand jury sitting in the Eastern District of Wisconsin returned a forty-four count indictment (Case No. 20-CR-30) against David Joel Quinones-Rios and twenty-five other codefendants. Quinones-Rios is charged in Count One of the indictment which alleges that he and others known and unknown to the grand jury conspired to possess with the intent to distribute and to distribute five kilograms or more of a mixture and substance containing a detectable amount of cocaine, a Schedule II controlled substance, in violation of Title 21, United States Code, Sections 846 and 841(b)(1)(A); and, Count Seven of the indictment which alleges that he and others known and unknown to the grand jury conspired to launder monetary instruments in violation of Title 18, United States Code, Section 1956(h).

21. On January 15, 2020, law enforcement officers executed a search warrant in relation to the above-referenced criminal complaint at a residential property located at GPS coordinates: 18.4068300. -67.173210, in Aguada, Puerto Rico, which had been identified as Quinones-Rios' residence. Codefendants who live nearby, including David Quinones-Quinones (Quinones-Rios' father), were arrested on January 15, 2020 as well. Since the issuance of Quinones-Rios' arrest warrant in this case, Quinones-Rios has eluded apprehension by law enforcement authorities and is a fugitive. Given the search of Quinones-Rios' residence and the apprehension of nearby coconspirators, there is reason to believe that Quinones-Rios is aware of his pending federal charges and has fled in violation of Title 18, United States Code, Section 1073 (Flight to Avoid Prosecution). There is also probable cause to believe that the information described in Attachment B will assist law enforcement in arresting Quinones-Rios, who is a person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

22. On January 16, 2020, your Affiant conducted a public search of Facebook.com and located the profile user name "**Rios Davito**" with url: <https://www.facebook.com/davito.rios.56> (i.e. **Target Account**). In addition, at the same time through a public Facebook Inc. website, your Affiant located the corresponding Facebook ID for the **Target Account**. Based upon a comparison with known photographs of Quinones-Rios maintained by the U.S. Marshals Service and Drug Enforcement Administration (DEA), publicly posted images of the user of the **Target Account** appear to be that of Quinones-Rios. Furthermore, the Facebook user name, "**Rios Davito**" and the url containing "**davito.rios.56**," appear to be derivations of Quinones-Rios' name. Based upon the investigation and contact with case agents, your Affiant is also aware that David Quinones-Rios uses the nickname "Davito" which is also contained within the account name.

23. Your Affiant was also able to publicly view images associated with the **Target Account's** timeline. Your Affiant located a post timestamped on January 2, 2020, depicting David Quinones-Rios standing with co-defendant Hector Yamil Rodriguez-Rodriguez.

24. The account "**Rios Davito**" initially remained active until the last post on January 15, 2020, at approximately 1:57 a.m. that stated, "Every day that passes comes out a piggy every day i count with less."

25. On January 24, 2020, Pen Register and Trap and Trace orders were signed by the Honorable Magistrate Judge Nancy Joseph. Your affiant served Facebook, Inc. with the orders. On January 27, 2020, Facebook provided a notification to your Affiant that indicated another user attempted to message Quinones-Rios; however, no IP Addresses were generated, suggesting no activity on his account since January 15, 2020 (the date all arrest warrants were executed).

26. Subsequently, On March 23, 2020, Pen Register and Trap and Trace Extension orders were signed by the Honorable Magistrate Judge William Duffin. Your Affiant served Facebook Inc. with the orders.

27. On April 12, 2020, your affiant received multiple notifications from Facebook, Inc. A review of these notifications revealed that the **Target Account** messaged other Facebook users that generated IP Addresses. This activity has occurred every few days through the present.

28. Based on your affiant's training and experience in locating and apprehending potentially violent fugitives, the data being sought by this warrant will assist in locating Quinones-Rios. Because successful apprehensions, particularly of violent fugitives, often rely on the element of surprise and on taking the fugitive by unaware, it is often necessary to attempt an arrest during nighttime or the early morning hours, when most people are sleeping. Further,

apprehension tactical plans often change at the last minute based on unexpected movements or other behavior of the target. Therefore, I cannot predict in advance when this data would need to be accessed, and would need access to the data at all times of the day or night in order to ensure a safe and successful apprehension.

29. As of the date of this affidavit, Quinones-Rios' whereabouts remain unknown, and the arrest warrant remains active.

### **CONCLUSION**

30. Based on the facts set forth in this Affidavit, your Affiant submits that there is probable cause to believe that the subject accounts contain the fruits, instrumentalities, and evidence of the subject offense.

**ATTACHMENT A**

This warrant applies to information associated with the following Facebook username and user ID which is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered at 1610 Willow Road, Menlo Park, California.

User name **Rios Davito**, Facebook User ID: **100013585895525**.

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be disclosed by Facebook**

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. (“Facebook”), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the user ID listed in Attachment A from January 15, 2020, through the present:

- (a) All contact and personal identifying information, including **Rios Davito** corresponding to **Facebook ID 100013585895525**, **<https://www.facebook.com/davito.rios.56>**: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities from January 15, 2020 to the present;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them from January 15, 2020 to the present, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;
- (d) All profile information; News Feed information; status updates; links to videos,

photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, the user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (f) All other records of communications and messages made or received by the user, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;
- (g) All "check ins" and other location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (j) All information about the Facebook pages that the account is or was a "fan" of;
- (k) All past and present lists of friends created by the account;
- (l) All records of Facebook searches performed by the account;
- (m) All information about the user's access and use of Facebook Marketplace;
- (n) The types of service utilized by the user;
- (o) The length of service (including start date) and the means and source of any

payments associated with the service (including any credit card or bank account number);

- (p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Facebook Inc. is hereby ordered to disclose the above information to the government within fourteen (14) days of service of this warrant.